Testimony of Benjamin Edelman

before the

United States House of Representatives
Committee on the Judiciary
Subcommittee on Courts, the Internet, and Intellectual Property

September 4, 2003

Benjamin Edelman
Berkman Center for Internet & Society
at Harvard Law School
<http://cyber.law.harvard.edu/edelman>

Baker House – Harvard Law School
1587 Massachusetts Avenue
Cambridge, MA 02138

Chairman Smith, Ranking Member Berman, Members of the Subcommittee:

My name is Benjamin Edelman, and I am a fellow at the Berkman Center for Internet & Society at Harvard Law School, where I write software to study the Internet. Among my research interests is the Internet's domain name system, and I have written a series of articles about flaws in the Whois system, about domain name registrants who exploit these flaws, and about possible means of detecting and preventing such exploits. My full biography and publication list are available at http://cyber.law.harvard.edu/edelman .

In the interests of full disclosure, let me pause to note that I previously worked for ICANN. I designed and operated webcasts of fully a dozen ICANN's meetings – so that anyone interested could watch, read, and even ask a question from home or office, without traveling to a far-flung meeting site. In 2000-2001, I also briefly served as a consultant to ICANN as to technical issues associated with the introduction of new top-level domains as well as with certain security and competition concerns.

Today the subcommittee considers the accuracy of the Whois database, and the role of the Department of Commerce, ICANN, registries, and registrars in assuring the accuracy of Whois data.

My bottom line:

As the DNS is currently structured, registrants are under only an honor system to provide accurate Whois data. Meanwhile, it makes no economic sense for registrars to enforce Whois accuracy. The result is that in terms of accuracy, when compared with other compilations of public data (such as driver's licenses and trademark registrations), the Whois database is substantially fiction.

Despite years of inquiry by this subcommittee, in addition to numerous ICANN working groups and other discussions, intentionally invalid Whois data remains widespread. But failure to solve this problem so far doesn't mean the subcommittee must give up. Instead, new efforts at detection could better find invalid domain names, while new incentive systems assure that registrants provide accurate data and that registrars confirm that they do so.

My specific suggested incentives include 1) a reduction in the lenience of opportunity to "cure" intentionally invalid data, 2) for registrants with multiple domain names with intentionally invalid data, forfeiture of all domains when any are to be cancelled, 3) statistically valid surveys of registrars' Whois accuracy, with public reporting of each registrar's accuracy, 4) public reporting of Whois accuracy complaints and their dispositions, and 5) financial and other penalties to registrars with poor Whois accuracy records.

Scope of the Problem of Invalid Whois Data

The Internet's domain name system (DNS) currently includes approximately thirty million domain names within the top-level domains of .COM, .NET, and .ORG. Under ICANN policy, passed on to domain registrants through contracts via registry and registrar, each of these domains must report the name, address, telephone number, and email address of its technical and administrative contacts, as well as the name and address of the its registrant. This information must be published via the so-called "Whois" database operated by domain name registrars.

It has long been known that a large number of domain names offer invalid Whois contact information. In some instances, the invalidity may be unintentional; registrars' data systems occasionally corrupt registrant contact information, and registrants (especially non-native English speakers) might misunderstand registration forms. In general, though, invalidity is thought to be intentional, reflecting registrants' desire to keep their identities confidential. This inference is particularly strong when Whois data is obviously intentionally invalid ("123 Main Street" or "0 Does Not Exist Lane"), when invalid Whois data is combined with controversial content (pornography, cybersquatting, etc.), or when the invalid information and associated web sites are clearly the work of sophisticated registrants.

In the past, some have attributed Whois accuracy shortfalls to difficulty in determining whether specified addresses are valid. After all, if a registrar cannot determine if a given address is accurate, the registrar cannot enforce accuracy requirements. However, automated systems are increasingly well able to cross-check registrant name, address, and postal code, all with minimal delay and low cost, at least as to registrations in industrialized countries. A new service called Fraudit (from a DNS service provider called Alice's Registry[1]) performs precisely these functions, using only publicly-available databases. Credit card verification software typically uses similar methods, and registrars have been using card verification software for some time in order to reduce "chargeback" penalties and confirm validity of customer credit cards. However, I know of no registrar currently using these methods to prevent invalid Whois data.

Using a variety of methods of locating suspicious registrations, my prior research identifies thousands of domains with intentionally invalid Whois data. For example, in my May 2002 *Large-Scale Intentional Invalid Whois Data: A Case Study of "NicGod Productions" / "Domains For Sale"*,[2] I identified a total of 2,754 domains registered by a single registrant – but using addresses in at least ten countries, registered via at least eleven registrars. Similarly, my January 2003 *Large-Scale Registration of Domains with Typographical Errors*[3] reports more

[1] http://www.ar.com
[2] http://cyber.law.harvard.edu/people/edelman/invalid-whois
[3] http://cyber.law.harvard.edu/people/edelman/typo-domains

than 8,800 domains registered by a single registrant using at least six pseudonyms, using addresses in at least six countries, and using at least four registrars.

Intentionally invalid Whois data is often associated with other controversial registration practices. This is perhaps not surprising – after all, registrants with something to hide are particularly likely to conceal their true contact information. My *NicGod* research found clear evidence of bulk registration of domains previously used by other registrants, then allowed to lapse (typically mistakenly, e.g. by administrative error), subsequently captured by NicGod, which then attempts to resell them to their original registrants after markups on the order of 5000%. My *Typographical Errors* research found registrations of strings that are small variations on well-known marks (e.g. cartoonneetwork.com [sic]), and the resulting domains were typically redirected to sites offering pornography, online gambling, filesharing, or other controversial materials. These are troubling practices – practices which force small business owners to pay thousands of dollars to retain the domains they previously used, and practices which expose Internet users to pornography as a penalty for small mistakes in typing URLs.

Incentives for Registrants to Provide Accurate Data

That registrants provide invalid Whois data should perhaps come as no surprise. After all, domain name registrants have only limited incentives to provide accurate Whois data.

1. Accurate Whois data is not necessary in order to pay for a domain name. Even when contact information is cross-checked with credit card records at the time of domain registration, it is typically possible to modify contact information subsequent to registration.

2. Registration agreements, typically accepted by registrants by pressing an "I agree" or similar button during the domain name registration process, oblige a registrant to provide accurate Whois information. But few registrants typically read these agreements, and the format of these agreements rarely places special emphasis on Whois accuracy.

3. Even when registrars send periodic reminders that Whois data must be kept up to date, as is required under ICANN's Whois Data Reminder Policy,[4] registrants are likely to ignore the reminders. This too is no surprise – particularly since Whois reminders are widely thought not to be supported by active investigation or enforcement.

[4] "At least annually, a registrar must present to the registrant the current Whois information, and remind the registrant that provision of false Whois information can be grounds for cancellation of their domain name registration. Registrants must review their Whois data, and make any corrections." http://www.icann.org/registrars/wdrp.htm

4. When a registrar receives a complaint as to the accuracy of a registrant's Whois data, the registrar typically grants the registrant an opportunity to cure the problem by correcting the invalid entry. Anticipating this opportunity, a registrant need not offer accurate information in the first instance. Instead, the registrant can provide invalid Whois data, to be corrected only upon complaint. In addition, some registrants provide a series of invalid contact names and addresses, a problem recently faced by staff of the OECD.[5]

In short, the current registration scheme fails to set incentives for registrants to provide accurate Whois data. The system provides no incentives for registrants to provide accurate data in the first instance – for registrants always receive an opportunity to cure invalid entries, without penalty. Furthermore, the system allows bulk registrants to sacrifice a disputed domain rather than share their true identities – for domain cancellations are limited to the specific disputed domains and do not extend to other domains registered by the same registrant using the same invalid Whois data.

The following modifications would correct these incentive problems

1. When a registrant's Whois data is found to be intentionally inaccurate, penalize the registrant in some way before (or instead of) offering an opportunity to correct the error. The penalty could consist of charging a fee for investigation, or forfeiting some period of prepaid registration service.

2. When a given domain name is to be cancelled for offering invalid Whois data, also cancel all other domain names registered with identical invalid Whois data.

Incentives for Registrars to Assure Accurate Data

Registrars' failure to enforce Whois accuracy is also predictable, for registrars face equally limited incentives to provide accurate Whois data.

1. Registrar contracts with ICANN oblige registrars to include certain language in their contracts with registrants, asking registrants to provide accurate Whois data.[6] But this requirement extends only to language in registration agreements – not to actual efforts at enforcement. Neither do other sections of registrar contracts with ICANN require specific enforcement procedures as against registrants who provide invalid Whois

[5] "Cybersquatting: The OECD's Experience and the Problems It Illustrates with Registrar Practices and the 'Whois' System" http://www.oecd.org/dataoecd/46/53/2074621.pdf

[6] "Registrar shall require all Registered Name Holders to enter into an electronic or paper registration agreement with Registrar including at least the following provisions …" http://www.icann.org/registrars/ra-agreement-17may01.htm#3.7.7

data.[7] In fact, ICANN specifically allows registrars to maintain domains even in the face of intentionally invalid Whois data constituting a material breach of the domain registration agreement.[8]

2. For failure to assure Whois accuracy, registrars face only a toothless sanction from ICANN, and ICANN isn't even making meaningful use of this approach. Pursuant to ICANN's April 3, 2003 advisory to registrars,[9] and as took place in September 2002,[10] ICANN may present a registrar with a formal notice of breach if, in ICANN's view, the registrar "appears to routinely ignore reports of inaccurate and incomplete contact data in its Whois database." However, only one such notice has been issued to date; it reported inaccuracies in only seventeen domains; its recipient was a registrar not typically thought to harbor particularly egregious cases of invalid Whois data; the only resulting sanction was brief public embarrassment for the registrar, without financial penalty. Registrars are unlikely to respond to such sporadic enforcement by ICANN.

In contrast, registrars face clear incentives to allow inaccurate Whois data.

1. The costs of inaccurate Whois data fall not on registrars but on others – on law enforcement officials, on consumers, and on those wishing to pursue copyright, trademark, and other claims against domain name registrants.

2. A registrar that enforces Whois accuracy requirements faces increased costs relative to a registrar that ignores Whois accuracy. Increased costs include staff time to seek out errors and respond to customer complaints, as well as software to automate these processes.

3. A registrar that enforces Whois accuracy requirements may face lost revenue by driving certain customers to other registrars. In particular, large registrants with systematic intentionally invalid contact information (such as the registrants described in my *NicGod* and *Typographical Errors* research) are likely to select registrars that allow or tolerate invalid contact information.

The following policy changes would correct these incentive problems:

1. ICANN could commission audits of Whois accuracy, using statistically valid methods to examine a significant sample of domains. Results would be tabulated and published on a per-registrar basis, allowing comparisons of Whois accuracy among registrars.

---

[7] e.g. "take reasonable steps to investigate" – http://www.icann.org/registrars/ra-agreement-17may01.htm#3.7.8

[8] http://www.icann.org/announcements/advisory-03apr03.htm

[9] http://www.icann.org/announcements/advisory-03apr03.htm

[10] http://www.icann.org/correspondence/touton-letter-to-beckwith-03sep02.htm

2. ICANN could use the results of Whois accuracy audits to present registrars with formal notices of breach of their contracts with ICANN.

3. If formal notices of breach fail to encourage registrars to improve their performance on Whois accuracy audits, ICANN could implement a system of graduated financial sanctions, consistent with ICANN's practice for registry service level agreements.[11]

4. ICANN could post periodic statistics as to Whois Data Problem Reports, Registrar Problem Reports, and registrars' actions taken in response to these complaints.

All registrars would face these policy changes simultaneously and equally. Across-the-board enforcement of Whois accuracy would prevent registrants from switching registrars to avoid Whois enforcement efforts.

Privacy Concerns Reflect Misguided Overemphasis

In response to calls for increased Whois accuracy and enforcement, some have raised privacy concerns.[12] Their typical worry is that an emphasis on Whois accuracy would purportedly prevent individuals from registering domains for purposes that are in some way controversial yet simultaneously commendable (e.g. political dissent, whistle-blowers, or other anonymous speech).

Policymakers rightly encourage the use of the Internet for activities legitimately requiring anonymity. However, such activities are in no way incompatible with accurate Whois data. Domain registrants who wish to keep their name and address confidential can register names through one of several third-party services specializing in privacy protection[13] or can register names through an attorney or other representative. It is not necessary to sacrifice Whois accuracy in order to preserve the possibility of anonymous publication on the web.

Distinct from the privacy concerns typically offered in response to calls for Whois accuracy, are concerns as to publication of truthful email addresses, for fear of receiving unsolicited email. In the past, such emails have included offers from registrars and web hosting companies. More recently, email worms and viruses have proven particularly disruptive. I am sympathetic to these concerns, but the proper response is not to discard all calls for Whois accuracy. Indeed, email concerns in no way lessen the need for accurate registrant name, address, and telephone information. Instead, those who find bulk email problematic can route their email through any of various mail filtering services, or can rely on temporary "alias" email addresses. Certain registrars already offer this email alias feature,

[11] e.g. http://www.icann.org/tlds/agreements/name/registry-agmt-appe-02jul01.htm
[12] e.g. Electronic Privacy Information Center – Whois. http://www.epic.org/privacy/whois/
[13] e.g. GoDaddy's Private Registration service, https://registrar.godaddy.com/dbp.asp?isc=&se=%2B&pl_id=1&prog_id=GoDaddy

typically at no additional charge.[14] In any case, recent research indicates that Whois records are not a significant source of spam.[15]

Trends in Registrar Compliance with ICANN Policies

I understand that the subcommittee is also concerned about the possibility that certain registrars systematically tend not to comply with relevant ICANN policies. In particular, despite obligations under the Registrar Accreditation Agreement, certain registrars apparently ignore selected UDRP judgments calling for transfer of domains away from the registrars and their registrant customers. New York attorney Martin Schwimmer publicly raised this issue in a blog entry of June 4, 2003,[16] and I have subsequently attempted to quantify the scope of the problem in my *Compliance with UDRP Decisions: A Case Study of Joker.com*.[17] I have found significant evidence that registrar Joker.com, perhaps among others, systematically fails to abide by its contractual obligation to transfer domains subsequent to orders received from UDRP panels.

To assure that registrars comply with their contractual obligations to ICANN, ICANN could establish a procedure for formally receiving, processing, and acting on complaints against registrars, ultimately upon threat of termination of an offending registrar's Accreditation Agreement. At present, ICANN's investigative procedures are ad hoc, and many complaints therefore fall through the cracks – with extended delays before ICANN takes action, if it does so at all. A more formal method of passing complaints to ICANN – complete with web-based publication of complaints, status, and disposition – would assure that ICANN acts promptly and transparently in resolving these situations.

The Special Problems of .US

The Department of Commerce has a special ability to shape policy in the United States' country-code top-level domain, .US. In particular, the DoC has a direct contractual relationship with .US registry Neustar, allowing DoC to directly specify .US policies. (In contrast, DoC's influence over policies in .COM, .NET, etc. require passing through DoC's Memorandum of Understanding with ICANN and subsequently through ICANN's policy-making process.) In this context, it is particularly desirable to assure that .US Whois rules and associated registration policies are fully in order.

---

[14] e.g. http://www.namescout.com/master/privacyfeatures.asp

[15] "Addresses posted in … Whois domain name registries … did not receive any spam during the six weeks of the investigation." http://www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm "Domain name registration does not seem to be a major source of spam." http://www.cdt.org/speech/spam/030319spamreport.pdf .

[16] http://trademark.blog.us/blog/2003/06/04.html#a646

[17] http://cyber.law.harvard.edu/people/edelman/udrp-compliance

.US Whois Policy

Neustar's .US Policies page[18] makes no mention of a .US policy as to Whois accuracy or registry procedures for assuring Whois accuracy. NeuStar's Registration Review Policy[19] references "Accuracy of information," but places this section at heading six on page three of a PDF file (easy for registrants to miss) and fails to use the word "Whois" to make clear to registrants what specific information is at issue. Improvements in these areas are necessary to assure .US's position as a leader in Whois accuracy.

.US Nexus Requirements

Closely related to .US Whois rules are .US nexus requirements for registration. Under the .US Nexus Requirements,[20] .US domains may be registered only by 1) US citizens or residents, 2) US entities or organizations, and 3) foreign entities or organizations with a bona fide presence in the US. In practice, however, .US domains are registered by a variety of entities meeting none of these criteria. Furthermore, these entities often register a large number of domains – as many as 800 per registrant, in my research – and their domains often infringe on the marks of others. These practices are documented in my *Survey of Usage of the .US TLD*.[21] However, despite discussion list coverage of this research, as well as numerous personal emails from concerned citizens to staff at the Department of Commerce and at Neustar, I gather these registrations remain in effect, in many instances with new invalid Whois information replacing the old.

If existing procedures fail to separate US from non-US registrants – on the basis of what could initially have been presumed to have been truthful registrant contact information – their ability to perform the more subtle task of separating valid Whois contact data from invalid entries ought to be very much in question. Here too, improvement likely requires setting appropriate incentives – requiring Neustar to face a penalty when it allows the registration of scores of domains with invalid Whois data or with invalid nexus qualifications.

The Unavailability of the .US Zone File

The Department of Commerce's agreement with Neustar apparently fails to provide the public with access to the .US zone file (the list of all registered .US domain names). Zone files are essential for conducting research as to trends in domain registrations, and public access to zone files is therefore a cornerstone of all ICANN contracts with gTLDs. However, Neustar reports that the DoC has failed to provide for such access under its .US contract with Neustar, and Neustar staff refuse to distribute the file to the public until the DoC and Neustar agree on terms for doing so. As a result, research and public critique of .US registrations and policies are rendered considerably more difficult, and it was

[18] http://www.nic.us/policies
[19] http://www.nic.us/policies/docs/registration_review_policy.pdf
[20] http://www.nic.us/policies/docs/ustld_nexus_requirements.pdf
[21] http://cyber.law.harvard.edu/people/edelman/dotus

only with considerable additional effort that I was able to conduct the *Survey* referenced above.

Lack of Related Efforts by the .US Policy Council

.US policy is to be set in consultation with a .US Policy Council, formed by Neustar in 2002. However, the status of this Council is unclear, with no meeting minutes posted since January 2003.[22] My sense is that this period has brought a similar lack of forward progress on .US Whois accuracy, nexus requirements, zone file availability, and other .US policy issues.

[22] http://www.neustar.us/policycouncil

Large-Scale Intentional Invalid WHOIS Data:
A Case Study of "NicGod Productions" / "Domains For Sale"

[Overview - "Domains For Sale" - Types of WHOIS Errors - Specific Domains - Summary Statistics - Conclusions - Policy Implications - Motivation]

Overview

In recent years, many Internet users have become aware that domain name registrants do not always offer accurate contact information. The distributed "WHOIS" database storing and distributing this contact data is generally thought to be important for correcting technical errata, resolving disputes over domain name allocation, and holding web site operators responsible for the content they distribute. A series of contracts, from ICANN to registrars to registrants, requires that contact data be complete and accurate, but nonetheless certain registrants fail to properly provide the required contact information.

While many WHOIS errors likely result from accidental error in data entry or data processing, certain registrants have been found to intentionally provide systematically inaccurate contact information to registrars for inclusion in the WHOIS database. Such fraud can include the entry of invalid street addresses and phone numbers, i.e. contact information that in fact reaches no one, or it can instead offer as the purported registrant of a domain some third party in fact wholly unrelated to the domain.

In recent research, I have documented 2754 domains reregistered by one particular firm known for its widespread use of invalid WHOIS contact information. The majority of these domains redirect users to a single web page displaying a list of links to content that is, by and large, unrelated; the remaining domain names provide access to sexually-explicit images. While this research is by no means exhaustive -- other firms likely follow similar registration practices, and still others make numerous invalid registrations and reregistrations that no doubt differ in various ways -- a review of these specific registrations as well as their general characteristics may be helpful in understanding the behavior at issue.

Note that this research is focused specifically on large-scale domain registrations. I do not address the questions of privacy, spam, and consumer protection raised by publication of individual registration data in the WHOIS database.

A Case Study: "Domains For Sale" Reregistrations by an Undetermined Registrant

Recent testing reflects that a firm calling itself "NicGod Productions" and "Domains For Sale" (henceforth, "NicGod") operates at least 2754 domain names that by and large redirect to a page that offers a list of links unrelated to the requested domain. A subset of NicGod's domains offer sexually-explicit images on a paid subscription basis.

NicGod's 2754 domains include a wide variety of character strings. The vast majority of domain names explicitly suggest specific content other than what is present on the subsequent list of links -- for example, angry-kids.com, californiastateuniversity.com, doctorjohn.com, polygram-us.com, reform-party-usa.org, and winthrop-police.com.

It seems that most or all of NicGod's domains were previously held by other registrants. According to archive.org, at least 1844 (67.0%) of NicGod's domains previously offered HTML titles suggesting the availability of other content, precisely indicating that the domains were previously put to another use before registration by NicGod. Some 246 (8.9%) of NicGod's domains continue to be listed in Yahoo, in categories reflecting the prior availability of content other than the current NicGod listing of links. Similarly, some 2170 (78.8%) of NicGod's domains are mentioned on one or more other pages, as reported by Google; these many outside references further suggest that the NicGod domains previously hosted other content. In this regard, NicGod's registration practices seem to be similar to those documented by this author in his April 2002 Domains Reregistered for Distribution of Unrelated Content: A Case Study of "Tina's Free Live Webcam".

A review of the current registrants of domains previously held by NicGod suggests that certain registrants, among them the major American firms of Hewlett-Packard and AOL, are coming to hold certain domains held by NicGod as recently as March of 2002. These firms may be purchasing the domains at issue from NicGod or may be using a UDRP or similar challenge to obtain the domains.

Update: This author attempted to contact NicGod at one of the phone numbers provided in WHOIS contact records. In a return call of four days later, the author learned that a randomly-selected NicGod-registered domain was available for $1200 (asking price) and could be transferred within 24 hours. The NicGod representative suggested payment via an escrow company, Paypal, or Afternic, noting that Afternic would charge a $100+ fee that he thought to be excessive. The NicGod representative responded to complaints about the proposed fee by reporting the randomly-selected domain's popularity in search engines Lycos, Hotbot, and Altavista and further noting that the domain received, in his experience, 200 or more "type-in" requests per day. When asked about the minimum price he had ever accepted for a domain name ("to avoid a loss" as he put it), the representative said $550 was his minimum, and when asked about his identity, he said he had "no secrets" and that his name was in fact Allen Ginsberg, notwithstanding that this is also (but, he seemed to suggest, only coincidentally) the name of a famous poet. The NicGod representative spoke fluent English in a heavy accent that this author found consistent with the hypothesis of Eastern European national origin. Caller ID was blocked on his incoming call. (May 15, 2002)

Update: I have added nearly 1500 additional domains currently or recently registered to NicGod, increasing the count of domains documented here from 1278 to 2754. (June 3, 2002)

WHOIS Errors and "Tricks": NicGod's Methods for Keeping Its Identity Secret

A review of NicGod registration practices shows a variety of techniques that seem to be used to keep secret the identity, location, and contact information of the NicGod staff.

The NicGod domains are notable for their wide variety of registration methods and purported contact locations. NicGod's domains use a total of eleven distinct registrars; leading registrars are Bulkregister (1294 domains), Dotster (379), The Registry at Info Avenue (285), eNom (154), Namescout (113), and iHoldings / dotRegistrar (62). Furthermore, NicGod provides at least nine distinct countries for registration of its various domain names, including Armenia, Bulgaria, Canada, Estonia, Germany, Hong Kong, the Netherlands, Russia, the Ukraine, and

the United States. A series of investigations has shown various of these addresses to be invalid. (International Herald Tribune, Detroit News Online / Bloomberg News, Radio Free Europe).

In addition to using a large number of invalid addresses for the registration of its domains, in many instances NicGod seems to enter the names of one or more well-known individuals as the purported registrant of its domains. For example, some 425 NicGod domains purport to be registered by Allen Ginsberg, also the name of a deceased American poet. For other domain registrations, NicGod uses a variety of company names -- including "Domain ForSale," "Grafikal Kompilations," "Merkus, Matching," "Triple Zero Networks," and "Ugol Hostmaster." An OECD report further alleges that in some instances NicGod uses or previously used as the registrant name for one domain the prior registrant's name from another domain -- causing substantial confusion as to who is responsible for NicGod's registrations.

Many of the domains registered by NicGod offer a telephone and fax contact in the United States. The specified phone number is a voice mail box in the 309 area code assigned to Bloomington, Illinois. Documentation gathered by the OECD suggests that NicGod may purchase this service from an Illinois voice mail firm; in this case, NicGod itself may nonetheless have no actual presence in Illinois.

Data collected by Patrick Jones of UDRPlaw.net suggests that NicGod has faced at least 27 challenges under the Uniform Domain-Name Dispute Resolution Policy (UDRP) but has in every instance failed to respond to complaints. It is possible that staff of NicGod would prefer to forfeit their domains under the UDRP, rather than reveal their identity by responding to a UDRP complaint; alternatively, staff of NicGod may not receive UDRP complaints precisely as a result of the invalid contact data provided by NicGod to its registrars.

Of course, even NicGod's methods may ultimately prove inadequate for keeping secret its identity. Most or all NicGod domains are hosted at dslextreme.com, an ISP in Canoga Park, California; it is possible that this firm knows the true identify and location of NicGod, information that it might have obtained in the course of billing or customer support. Alternatively, any of NicGod's registrars might know the firm's identity location from similar interactions. It is possible that any or all of these firms might disclose known information on the basis of a subpoena or other request. A Detroit News Online / Bloomberg News article suggests that the individual behind "NicGod Productions" may be Emil Lazarian, an 18-year-old Armenian exchange student.

Specific Domain Registrations with Invalid Contact Data

In recent testing and archiving, I have prepared a listing of a total of 2754 distinct domains that are (or recently were) registered to (or by) NicGod, and that likely offer (or recently offered) invalid contact data.

For each domain, I have attempted to obtain a variety of information including:

- Current title of default web page (as of May-June 2002)
- Date of domain registration by current registrant, when available from registrar; name of current registrar

- Prior page title, when available from archive.org (as of approximately January 1, 2000)
- Prior META DESCRIPTION and KEYWORDS tags, when available from archive.org (as of approximately January 1, 2000)
- Current Yahoo category, when available from Yahoo (as of May 2002)
- Other pages referencing or linking to domain, when available from Google (with counts as of May-June 2002)
- The number of times the domain's default web page was accessed by Alexa users between December 2001 and May 2002, with rank data when available
- The domain's registrant and administrative contact of record (as of May 2002)
- Access to page archives, when available from archive.org

The results of this data collection effort are freely and publicly available. Due to the large size of the listing of results, the listing is provided in sections by first letter of domain name:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z numbers

Summary Statistics

Of the 2754 distinct domains registered to NicGod, 2027 (73.6%) currently point to listings of links with pop-up advertising and possible click-through sponsorship. Of the remaining 166 domains, at least some have been transferred to other registrants (among them AOL and HP), and at least 43 offer sexually-explicit images.

According to current testing in Google, 2170 of NicGod's domains (78.8%) are mentioned in one or more web pages (as via a link or a textual reference to the domain name).

Yahoo continues to classify 246 of NicGod's domains (8.9%) into its hierarchical directory categories. In a casual inspection, none of these categories seems to properly characterize the content available from NicGod.

Archive.org reports that at least 2027 (73.6%) of NicGod's domains previously contained a title suggesting the availability of other content.

NicGod uses at least eleven different registrars (primarily Dotster, Bulkregister, and Namescout) and uses multiple registration addresses in at least nine distinct countries. Contact information in some registrations invokes the names of well-known individuals who are deceased as well as unaffiliated with NicGod.

Of NicGod's domains, Alexa toolbar logs reflect that the most popular were ITLIBRARY.COM (previously a resource about information technology) and ASCGAMES.COM (a computer game developer site). In the past six months, these sites received 131788 and 59361 accesses, respectively, from users of the Alexa toolbar -- making them, at least among Alexa users, the 3161th and 6877th most popular sites on the web. A total of 75 of NicGod's domains received more than 100 requests from Alexa users in the past six months -- suggesting that many of NicGod's domains were and remain relatively popular.

Possible Conclusions

While the data linked above is but a single case study of what is known to be a more widespread phenomenon, it is nonetheless possible to draw certain conclusions on the basis of work completed to date. Possible conclusions include the following:

- There exist substantial numbers of registrations with intentionally-invalid WHOIS contact information, and at least some registrants take significant deliberate steps to obfuscate their true identities and locations.
- Of registrants providing intentionally-invalid WHOIS contact information, at least some register and hold large number of domains.
- The problems with DNS are interrelated in the sense that those who register large numbers of domains with invalid WHOIS contact information may also engage in other activities of concern. For example, registrants offering invalid WHOIS contact information may tend to be the same registrants who reregister large numbers of domains for the distribution of unrelated and/or sexually-explicit materials, or who offer sexually-explicit material on domain names that do not immediately suggest the availability of such materials.
- Links and other online references continue to point to domain names even many months after those domains have come to host content inconsistent with the suggestion of the linking or referencing pages. This phenomenon holds both for relatively small linking entities (i.e. ordinary web pages) as well as large firms (such as Yahoo).
- The domains registered by NicGod are not "forgotten" or "unimportant." Indeed, many of these domains receive or previously received many thousands, if not millions, of accesses per year.

Future Work, Discussion, and Policy Implications

This work has focused on only several hundred registrations by a particular single firm. While that firm is in some circles notorious for the invalid data it enters into the WHOIS database, it would be desirable to collect additional data so as to better understand the scope of the problem. Unfortunately, large-scale analysis is difficult because it is in many instances time-consuming, difficult, and costly to determine whether or not a given contact is in fact invalid. Future work will seek to develop additional automated methods for verifying telephone numbers, for cross-checking telephone numbers with street addresses, and for otherwise recognizing suspect trends in WHOIS data. To this end, the author welcomes submission of additional examples of domains with intentionally-invalid contact information; send such submissions to the author.

While a full policy analysis is beyond the scope of the current project, available data suggests that existing work by registrars and ICANN has been unsuccessful in assuring the accuracy of WHOIS data. Instead, systematic errors have remained over time, and known-abusers have continued to register at least hundreds of domains without providing valid contact information.

In this context, ICANN's recent Registrar Advisory Concerning Whois Data Accuracy seems arguably too limited to fully and efficiently address the entire problem at hand. Instead, when a given domain is found to contain invalid contact information, and when this contact information is found to be intentionally invalid, a registrar might consider canceling *all* of that registrant's

domains rather than only a particular single domain. (To reduce the risk of error, the registrar would of course first use all available methods to attempt to contact the registrant. Furthermore, the domains at issue would initially be placed into some sort of "hold" status wherein they do not function on the Internet yet, for a limited time, can be returned only to the prior registrant but not to any other interested party.)

John Berryhill points out that improvements in the accuracy of the WHOIS database may have a dual effect -- first, as expected, to increase the ability of interested parties to learn the identity of the registrant of a given domain; second, to use that registrant's contact information to induce the registrant to transfer the domain to some other registrar or to otherwise defraud the registrant. (More information about domain name scams from the FTC.)

Some registrants may prefer to keep their contact information confidential. ICANN's Registrar Accreditation Agreement anticipates this possibility and therefore allows registrars to hold registrants' valid contact information in trust, while publishing in WHOIS only a placeholder address. Certain third-party firms provide a similar service. Note, however, that these intermediary services are separate and distinct from the large-scale intentional entry of invalid contact information that is the subject of this document's discussion and of which NicGod is an example.

Motivation

The purpose of this work is primarily academic -- to document the activity at issue for the benefit of those who seek to make policy decisions on related matters. In the context of ICANN's recent Registrar Advisory Concerning Whois Data Accuracy as well as associated Congressional hearings, the availability of this data and analysis is intended to be helpful to policy-makers and other interested parties.

This page is made available to inform discussion about the registration of Internet domain names. The data contained here is not intended for use for other purposes, and it should not be used for other purposes without first contacting the author.

In order to confirm the results of my testing and to attempt to obtain certain other information, I sent an email inquiry to various of the contacts listed in WHOIS records of domains registered by NicGod. I have to date received no reply to the questions posed. Comments from NicGod staff remain welcome, as are comments from others interested; with the permission of the author, comments may be posted or linked from this page as appropriate.

Ben Edelman

Last Updated: June 2, 2002 - Notify me of major updates and related work.

Large-Scale Registration of Domains with Typographical Errors

Benjamin Edelman - Berkman Center for Internet & Society - Harvard Law School

[Background - Specific Registered Domains - Analysis - Conclusions - Support This Work]

Abstract

The author reports more than eight thousand domains that consist of minor variations on the addresses of well-known web sites, reflecting typographical errors often made by Internet users manually typing these addresses into their web browsers. Although the majority of these domain names are variations of sites frequently used by children, and although their domain names do not suggest the presence of sexually-explicit content, more than 90% offer extensive sexually-explicit content. In addition, these domains are presented in a way that temporarily disables a browser's Back and Exit commands, preventing users from exiting easily. Most or all of the domains are registered to an individual previously enjoined by the FTC from operating domains that are typographic variations on famous names, and these domains remain operational subsequent to an injunction ordering their suspension.

Related Projects

- Domains Reregistered for Distribution of Unrelated Content: A Case Study of Tina's Free Live Webcam
- Large-Scale Intentional Invalid WHOIS Data: A Case Study of "NicGod Productions" / "Domains For Sale"
- Other work by the author

Background

This document investigates the registration of domain names that are minor typographical variations on well-known names in which the registrant lacks any legal right -- a practice sometimes called "typosquatting." The registrations reported here are also notable in at least three additional respects: First, many of these registrations feature invalid WHOIS data, failing to correctly report the name and contact information of a domain's registrant. (This is generally as described in the author's June 2002 Large-Scale Intentional Invalid WHOIS Data: A Case Study of 'NicGod Productions' / 'Domains For Sale'.) Second, many unexpectedly provide sexually-explicit content, even though their domain names do not suggest the availability of such content. (This is generally as described in the author's May 2002 Domains Reregistered for Distribution of Unrelated Content: A Case Study of 'Tina's Free Live Webcam'.) Finally, many make it difficult for a user to exit the site, blocking the ordinary operation of a web browser's Back and Close commands.

Of the domains reported here, most or all are registrations by John Zuccarini, doing business under multiple names including Mars Attack, Music Wave, Party Night Inc, Phayze 1 Phayze 2, and RaveClub Berlin. These many names (and their associated invalid WHOIS data) make it difficult to determine whether any given domain is in fact registered by Zuccarini, or whether domains were instead registered by others, but the author has endeavored to report only domains registered by Zuccarini.

Mr. Zuccarini's domain registrations have produced a series of legal challenges. According to a recent FTC press release, Zuccarini has faced seven federal court cases (including cases under the federal Anticybersquating Consumer Protection Act, or ACPA) and 56 UDRP arbitration proceedings (including UDRP challenges from Abercrombie & Fitch, American Airlines, the Backstreet Boys, Encyclopaedia Britannica, Hewlett Packard, Neiman-Marcus, Target, Voicestream, and Yahoo). (See Google listings of decisions from WIPO and the National Arbitration Forum.) In October 2001, the FTC brought suit against Zuccarini, challenging what the FTC called his "copycat" web addresses as well as his "mousetrap" techniques of preventing web users from exiting his sites. (The FTC's site provides their complaint, temporary restraining order, and preliminary injunction.) In May 2002, the FTC won a permanent injunction against Zuccarini (see the FTC's May 2002 update), barring Zuccarini from registering domains that are misspellings or other variations on third-party domain names, and further prohibiting him from obstructing a visitor's exit from a site. Nonetheless, eight months after the injunction was issued, the author's research demonstrates that the enjoined behavior continues: More than five thousand domains remain registered to Zuccarini or the company names he previously used; the overwhelming majority are typographical variations on well-known trademarks, popular phrases, and personal names. Most of Zuccarini's domains still

provide traps to delay or confuse a user's attempts to exit, and most still provide extensive sexually explicit content. The remainder of this document details these findings and their implications.

Specific Registered Domains

The author has located more than 8,800 domains registered, according to their WHOIS data, to John Zuccarini or his various company names (as identified by the FTC). This quantity is generally consistent with prior FTC reports of "more than 5,500" domains registered by Zuccarini; some domains may have expired in the interim, while others may have been added, and the FTC may not have been aware of all of Zuccarini's registrations.

The links below provide an alphabetical listing of the domains registered to Zuccarini. Each domain's entry includes selected additional information about it, including the domain's registrar, partial WHOIS data, and a categorization of the content posted on the domain's web site or post-redirection target.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z numbers

Due to the large number of domains registered by Zuccarini, the author has selected a sample of domains that reflect typographical errors on some of the most popular domain names and on domain names often used by children.

Highlights

Since the majority of Zuccarini's domain registrations are variations on other domain names, this site provides a system for users to help characterize the connections between Zuccarini's registrations and the domains he targeted with typographical variations. For example, the domain name "`woldmap.com`" (sic) is a variation on the name "`worldmap.com`." To submit such a variation to the database ont his site, follow the links marked "If this domain name contains a typo, suggest the name it derives from." The author will review all submissions and will post frequent updates to this site. In the future, the author may also post summary statistics of these results, and the author hopes to send messages to the registrants of the original domains to alert them to Zuccarini's variations on their domain names.

Reporting includes only Zuccarini names listed in .COM, .NET, and .ORG zone files of January 23, 2003 and March 21, 2003. Domains omitted from these zone files are omitted from the author's data collection systems and from his subsequent analysis. Pending UDRP decisions are one frequent cause of omission from zone files and therefore from the author's reporting; domains with pending UDRP decisions are omitted from zone files due to their *REGISTRAR-HOLD* status.

Analysis and Summary Statistics

Invalid WHOIS Data and Obfuscation. As described by the FTC, Zuccarini's use of multiple identities makes it difficult to confirm that the domains at issue are indeed his. Of the domains reported here, registrations are made in the name of John Zuccarini, Mars Attack, Music Wave, Party Night Inc, Phayze 1 Phayze 2, and RaveClub Berlin. Registrations are made from countries including the United States, the Bahamas, Burkina Faso, France, the Netherlands, and Switzerland. It is possible -- indeed, highly likely -- that Zuccarini holds numerous additional domains beyond those reported above. The author selected the domains reported here on the basis of multiple factors linking them to Zuccarini; relevant factors include WHOIS data, registrars used, DNS and web site configuration, and web content.

Registrars Used. Of Zuccarini's registrations reported here, most used registrars Joker.com (4,583 domains, 54.7% of those reported here) and Key-Systems GmbH (3,289 domains, 37.3%). As discussed below, these two registrars are both based in Germany, producing potential jurisdictional complications in the resolution of disputes regarding Zuccarini's registrations. Zuccarini also registered domains with Register.com (66) and Network Solutions (49). No other registrar registered more than ten of Zuccarini's domains.

Content Provided. At least 7,904 of Zuccarini's domains (90.0%) provide redirection to the site amaturevideos.nl, a sexually-explicit site that uses "mousetrapping" to prevent direct exit via a browser's Back button or via other ordinary browser commands. Provision of sexually-explicit content may be profitable to Zuccarini via at least two independent avenues: First, the FTC's complaint suggests that Zuccarini may have profited in part from affiliate fees paid to him when visitors make purchases from the sexually-explicit sites that are the targets of his redirects. Second, to the extent that Zuccarini anticipates selling domains to the registrants who hold the "real" sites on which Zuccarini's domains are variations, providing sexually-explicit content may increase the registrants' willingness to pay. (See related discussion in "Domains Reregistered for Distribution of Unrelated Content: A Case Study of "Tina's Free Live Webcam.") An additional 342 of Zuccarini's domains (3.9%) forward users to sites offering digital music downloads and tools; the domains that redirect to this content are variations on the names of products used to obtain digital music files.

Reconfiguration of Zuccarini Domains: Notwithstanding the court's injunction requiring the termination of Zuccarini's use of these domains, Zuccarini seems to maintain the ability to access and reconfigure his domain names. According to Verisign Registry WHOIS data, 7,547 of Zuccarini's domains (85.7% of those reported here) have had a configuration change since April 9, 2002, when the injunction was issued. Such changes are typically made only by a domain's registrant.

Domain Creation and Expiration Dates: According to data in WHOIS, the overwhelming majority of Zuccarini's domains were registered between August 1999 and March 2002. (However, fifteen domains were registered prior to August 1999. Eighteen domains were registered between April 2002 and August 2002, though none were registered since that time.) Most of Zuccarini's domains are slated to expire in 2003, but some will expire in January 2004, and a handful show expiration dates as late as May 2006.

Interaction of Typographical Variations with Trademarks: Mr. Zuccarini's registrations consist of variations both on trademarks and on generic terms. To the extent that Zuccarini's registrations are variations on trademarks (e.g. `verizonwierless.com`), the UDRP applies under its "confusingly similar" standard (section 4.a.i). To the extent that Zuccarini's registrations are variations on generic domains (e.g. `woldmap.com`), the UDRP does not apply, for the UDRP would not protect those generic domains on which certain of Zuccarini's domains are variations. Of course, there may as yet be no consensus (within the ICANN policy framework, or under governing national law) as to the rights of the registrant of a generic domain in typographical variations on that generic domain.

Conclusions

The continued operation of Zuccarini's domains suggests a possible failure of the various laws and policies to date brought to bear on his activities. UDRP challenges have proven effective for those domains targeted by specific UDRP actions. However, the UDRP entails a cost of several thousand dollars per domain (including both filing costs and attorneys fees), so UDRP expenses might well reach to the millions of millions of dollars due to the number of domains registered by Zuccarini. In this context, the FTC's en masse approach seems more likely to be effective. However, the FTC's action and the court's subsequent injunction seem to have failed to fully prevent the harm at issue, for Zuccarini continues to hold domains that seem to violate the court's injunction. Nonetheless, Zuccarini's current "mousetrapping" is somewhat less effective than his prior implementation, yielding fewer popup windows when a user attempts to close a Zuccarini site, suggesting that the FTC's injunction may have yielded improvement in this regard.

Jurisdictional issues may make the situation particularly difficult to resolve: Zuccarini has reportedly moved to the Bahamas (cite), from which extradition would likely be required to enforce a judgment of an American court. In addition, an American court may lack any way to order foreign registrars to take action, and Zuccarini's primary registrars (Joker.com and Key-Systems GmbH) are based in Germany. To improve compliance in the future, an American court might order specific actions by registrars and might send copies of its order directly to registrars (rather than relying on the defendant to do so, as explained in the court's permanent injunction). Even so, non-US registrars may refuse to comply. Concerned parties might seek to convince ICANN to address the situation -- perhaps by requiring registrars, under the terms of their accreditation agreements, to comply with orders of American courts. (The current Registrar Accreditation Agreement requires, in section 3.7.7.10, only that a registrar abide by orders from courts in the registrar's jurisdiction and in the jurisdiction of the registrant -- the latter provision effectively unusable in the face of heterogeneous and invalid WHOIS data.) Of course, such an

approach would raise jurisdictional problems of its own; American registrars might protest a symmetrical duty that required their submission to orders from non-US courts. Alternatively, the UDRP might be modified to better address the possibility of large-scale offenders with hundreds or thousands of domains -- avoiding the jurisdictional problems inherent in suits in national courts, but expanding the UDRP's evidentiary and procedural scope to accommodate the increased complexity of larger cases. For now, the jurisdictional provisions of existing policies allow Zuccarini to contest UDRP decisions against him (under UDRP rule 4.k) via suits in German courts; Zuccarini has contested rulings against him in claims brought by Toyota, Vanguard, and Classmates Online Inc., as documented in links 67-69 of UDRPLaw.net's appeals page.

Meanwhile, pending a widening of jurisdiction over registrars or of the UDRP, courts that seek to enjoin behavior like Zuccarini's may take certain actions to increase the likelihood of registrar compliance. Whenever possible, courts could list all the specific domains to be transferred, cancelled, or put on hold -- giving registrars complete clarity as to the requested action, rather than demanding that they determine which domains are held by a particular offender. With the help of plaintiffs' counsel and experts if needed, along with the power of discovery, a court might be better able to identify the offender's domains than would the registrars at issue. When invalid WHOIS data makes it particularly difficult to identify the offender's domains, bringing this process under the control of the court relieves the burden on registrars who, in the face of difficult decisions and uncertain obligations, might otherwise choose to do nothing. In addition, anticipating registrars' fear of ambiguity in the wording of an injunction, a court might list prohibited activities with ever-greater specificity. The Zuccarini injunction shows room for improvement in this regard: It prohibits "operating, publishing, or disseminating web sites or pages with domain names that are misspellings of other domain names" (clause L.1.) -- a restriction that might be alleged to leave open the question of what constitutes a "misspelling" and that might thereby discourage some registrars from taking action.

The FTC advises that individuals who believe they have been victimized by Mr. Zuccarini can register their complaints via a toll-free telephone call to 1-877-FTC-HELP (1-877-382-4357).

Support This W ork

Partial support for this project was provided by the Berkman Center for Internet & Society at Harvard Law School. The author seeks additional financial support to continue this and related projects. Please contact the author with suggestions.

Last Updated: April 6, 2003 - Sign up for notification of major updates and related work.
An earlier version of this article was posted in January 2003, offering an initial listing of approximately 5,500 domains registered by Zuccarini.

Survey of Usage of the .US TLD

[Introduction - Methodology & Results - Conclusions & Future Work]

Abstract: Recent policy changes allow registrations in .US with few restrictions. The author collects data about all known .US registrations, analyzing their registration patterns and usage. Certain registrants are found to register more than 2,000 domains each; these registrants may be gathering domains for commercial applications requiring many domains or for future sale, and large registrants (with ten or more .US domains) jointly hold a total of 46.4% of .US registrations to date. Non-Americans are found to register 7.0% of domains, and some of these registrations may violate .US registration restrictions that require nexus in the United States. The overwhelming majority of .US registrations as yet provide no original web content; working .US web sites are found to be clustered with certain registrars, while certain other registrars tend to register domains that offer no web content and domains offered for resale.

Introduction

In 1985, Jon Postel created a series of top-level domains for use by interested countries; among these so-called country-code top level domains ("ccTLDs") domain was .US, bearing the two-letter country code ordinarily associated with the United States. For more than a decade thereafter, .US registrations were generally permitted only within a strict hierarchy reflecting both geographic and organizational categorizations (i.e. www.k12.wa.us for the public schools in Washington State). However, the National Telecommunications and Information Administration of the US Department of Commerce in 1998 began a consultation process to consider a liberalization of the .US registration hierarchy, and in the spring of 2002 .US was opened for second-level registrations (i.e. cars.us) via newly-selected registry operator Neustar and competitive registrars.

Four months after the opening of .US to public registration, the author seeks to investigate usage to date of the .US space. Such investigations in part follow the model of the author's previous studies of domain names, quantifying top registrants, registrar market shares, warehousing, defensive registrations, and cybersquatting. Analysis further considers .US domains that may not comply with .US registration restrictions.

Methodology & Results

To analyze domain registrations and use, the author began with a full listing of all registered .US domain names. Many TLDs provide such a listing upon request, via a so-called "zone transfer" often accompanied by a license agreement; however, Neustar told the author that zone file is currently available only to .US registrars but not to the general public (email communications of May 21, 2002 and August 12, 2002). The author sincerely thanks a .US registrar, who prefers to remain anonymous, for providing the zone file so central to subsequent analysis.

The author used automated systems to collect data about each registered .US domain. From publicly-available WHOIS data, the author collected registrant name and organization, registrar, and date of registration, as well as the country of registrant and of administrative, billing, and technical contacts. The author further collected the title of each domain's default web page (when available).

Analysis uses the .US zone file of August 13, 2002, which includes a total of 307,788 distinct .US domains.

Results include the following five sections:

Registration Patterns of Top .US Registrants

Certain registrants were found to register a large number of .US names. For example, Bryon Uding of the American Spirit registered 2,494 .US domains, Bradley Norrish of Internet Registrations Worldwide registered 1,746, and Sanda Yackolow of Marblehead Consulting registered 1,500. The tables linked below summarize and detail .US registrations by registrants with ten or more .US domains.

.US Registrations by Top Registrants
.US Registrations by Top Registrants, with domain listings
Page 1, 2, 3, 4, 5, 6, 7, 8

Note that some "top registrant" listings reflect registrations in the name of a registrar. The author contacted representatives of certain registrars and was in most instances told that these registrations will in due course be modified to reflect registration by registrars' existing customers.

Inspection of the registrations of top registrants shows five notable categories of .US domains. The first three categories listed below are specific to the "us" string specifically, while the final two are consistent with open TLDs generally.

- *Geographic locations*. Some domains bear city names (for example, `albany-ny.us` and 929 other names registered by Gagan Patnaik), while others include both place names and product names (`bronxrealestate.us` and many of the 554 other names registered by Max Rinaldi).
- *Other US-specific content*, including content that is explicitly patriotic or otherwise related to the United States.
- *Other usages of "us."* For example, many domains use the string "us" to signify not "United States" but rather the first person plural objective pronoun. Examples include many of the 2494 registrations by Bryon Uding, such as `a-good-time-with.us` and `bargains-for.us`.
- *Defensive registrations*. Trademark holders have submitted a variety of registrations to prevent use of their marks by others. For example, Johnson & Johnson registered 783 .US domains including product names (childrenstylenolflu.us) and generics (allaboutkneesurgery.us); consistent with the author's prior investigation of defensive registrations, these domains do not provide web pages. Amazon took a different approach with the registration of sixteen names seemingly intended to help users who make typos or to prevent others from "typosquatting" on Amazon's marks; Amazon's .US registrations include `aamzon.us`, `amaozn.us`, and `amozan.us`, and these sites all redirect to Amazon's ordinary web site at amazon.com. Defensive registrations in .US include registrations by non-American firms such as Unilever (99 .US domains registered) and Emirates Airline (24).
- *General registrations of arbitrary strings*. As expected in an open TLD, .US domains include a large body of content of general registrations. Among top registrants, notable examples include most or all three-letter .us domains (`aaa.us` and so forth, including the overwhelming majority of Bradley Norrish's 1746 registrations), generic business names (`bookstore.us` and many others of Richard Leeds' 1,333 registrations), and sexually-explicit content (`all-animalsex.us` and 833 other domains by Silver Back Corp).

Registrations by Non-US Registrants

Certain .US domains were found to provide (in their WHOIS registrant and contact data) addresses outside the US. Under the .US Nexus Requirements (PDF), .US domains may be registered only by 1) US citizens or residents, 2) US entities or organizations, and 3) foreign entities or organizations with a *bona fide* presence in the US. To determine whether a foreign entity has such a presence, registration requirements specify consideration both of a registrant's ordinary lawful activities within the United States and of a registrant's offices or other facilities in the US.

The author knows of no automated means of confirming that a registrant in fact complies with nexus requirements; indeed, Neustar's Nexus Requirements document contemplates only occasional scans and spot checks. However, when a non-US registrant holds many .US names, the registrant may be particularly likely not to comply with stated nexus requirements; a non-US registrant holding dozens or hundreds of .US names, each pointing to an "under construction" site or an error message, might be thought more likely to be a domain warehouser or reseller than a foreign entity with a bona fide presence in the US. Accordingly, the author below reports those registrants who have registered 5 or more .US domains that each provide addresses outside the US for registrant address and for administrative, billing, and technical contacts. Of course, many of these registrations no doubt comply with Nexus Requirements, but at least some may reflect registration by a non-US individual or by a non-US organization without the required US nexus.

.US Registrations by Non-US Registrants

Of .US registrants with all contacts outside the US, some registrants registered many .US domains. Silver Back Corp (of Antigua and Barbuda) registered 834 domains including all-animalsex.us, alyssa-milano-gallery.us, alyssa-milano-naked.us, and alyssa-milano-nude.us; Global DNS Services (of the Netherlands) registered 474 domains including 11b.us, aanbieding.us, aanbiedingen.us, and adult-toy.us; B.Stone of the Netherlands registered 226 including afterparty.us, ahold.us, americangigolo.us, and americanpornstar.us. A total of 613 distinct registrants registered 5 or more domains with all contacts outside the US, and a total of 21,639 domains were registered with all contacts outside the US (7.0% of all .US registrations to date).

As detailed in the .US WHOIS FAQ, each .US domain includes a designation of its nexus code. Possible codes include C11 (US citizen), C12 (permanent resident of US), C21 (US organization), C31 (foreign entity or organization with bona fide US presence, regularly engaging in lawful activities in the US), and C32 (office or other facility in the US). As among .US registrations with all contacts outside the US, the table below reports the number of registrants providing each of these nexus codes:

	Number of .US Registrations (among .US registrations with all contacts outside the US)	Proportion of .US Registrations
US Citizen	3392	15.6%
Permanent Resident of US	751	3.5%
US Organization	1373	6.3%
Foreign Entity or Organization with Bona Fide US Presence, Regularly Engaging in Lawful Activities in US	12766	58.7%
Office or Other Facility in the US	2848	13.1%
No nexus data available in WHOIS	609	2.8%

Impermissible .US registrations (by registrants without the required nexus) may tend to take place within certain purported nexus codes. However, research to date has not identified nexus codes disproportionately used for this purpose.

Rate of Registration

WHOIS "Domain Registration Date" data provides information about the date of registration of each registered .US domain.

.US Registrations Per Day - chart and table

This data reflects that more than 56% of .US name were registered on or before April 30, 2002 -- in the .US

sunrise process. Since that time, approximately 1,000 .US domains have been added per day; this rate has remained roughly constant since June 1, 2002. Clear weekly trends reflect fewer registrations on weekends than on weekdays.

With approximately 308,000 domains registered through August 13, 2002 and a growth rate of 1,000 domains per week, extrapolation suggests a total of approximately 332,000 domains on January 1, 2003.

Registrar Market Share

Interested registrants obtain .US names through accredited .US registrars. The chart and table linked below summarize registrar market share to date.

.US Registrar Market Share - chart and table

This data reflects that leading .US registrars are Go Daddy (55,687.US names, 18.09% of registrations to date), Register.com (42,645, 13.86%), Verisign (38,578, 12.54%), Enom (27,437, 8.92%), and Directnic (16,740, 5.44%). Together, these five registrars sponsor 58.84% of .US registrations, while a total of 65 other registrars sponsor the remaining 126,661 .US domains.

Among the twenty largest .US registrars, 12 registered between 40% and 80% of their .US names during the .US sunrise. Certain other registrars did not participate in the sunrise; Wild West Domains registered its first domain on July 16, and Stargate Communications registered its first on July 27. Other registrars have registered only minimal names since the sunrise; such registrars include "Official US Domains" (6,245 sunrise registrations and 494 subsequently), Encirca (5,008 and 940), and Namescout (5,537 and 388). Additional details are available in the chart and table linked above.

Domain Usage & Registrar Specializations

The author attempted to obtain the default web page from each registered .US domain name, and when those pages were available, the author categorized available content into the groupings described below. Review and grouping of HTML page titles provided automated categorizations of the majority of tested web sites, while manual review was used for certain additional domains that could not be classified based on their ambiguous or omitted HTML page title.

	Proportion of all .US domains
Fails to provide a valid HTTP response ("cannot connect to server")	30.2%
HTML body is blank, provides a redirect, or includes "under construction," "coming soon," or similar	50.6%
HTML title or body contains an offer of sale	2.8%
Error message	1.1%
Uncategorized (includes domains with actual content)	15.3%

The large number of .US domains without default web pages, with blank pages, and with "under construction" or similar pages is consistent with the author's prior study of other top-level domains including .BIZ and the open country-code top-level domains of .CC, .TV, and .WS.

With knowledge of each .US domain's registrar, the author tabulated domain usage by registrar. As detailed in the table linked below, registrars vary greatly in their customers' usage of .US domains. Large .US registrars with relatively high estimated rates of provision of web content include Tucows (29.6%), Bulkregister (24.9%), Enom (23.5%), Go Daddy (17.9%), and Verisign (17.1%). Large registrars with substantially less frequent provision of

web content include Itsyourdomain (5.0%), Dotregistrar (6.2%), and Directnic (7.7%). Note, however, that certain large registrants can sway these estimates dramatically; for example, a single Bulkregister registrant provides substantially the same content on all of its 1,333 .US domains, but since these domains do provide actual web content, they count towards registrar Bulkregister's total and increase its "actual web content" proportion by 11.5%.

Registrants of certain registrars chose "under construction" pages for the overwhelming majority of their domains; for example, fully 83.1% of domains by registrar "Official US Domains" provided "construction" pages or were blank or redirects. However, registrations by certain other registrars disproportionately tended not to provide valid HTTP responses, perhaps because these registrars do not provide "under construction" pages or because their customers prefer not to use such pages; such registrars include R&K Global Business Services (87.3% of registered domains fail to provide a valid HTTP response), Encirca (88.5%), and Emarkmonitor (96.0%).

Domains with offers of sale tended to be clustered with registrars Domain Discover (42.5% of registered domains included an offer of sale on their default web pages), Directnic (11.0%), and CORE (18.9%). This result also primarily reflects clumping of registrants -- that these registrars each have one or several large registrants with many domains offered for sale.

Domain Usage by Registrar

Conclusions & Future Work

According to Neustar's Director of Policy and Business Development, the .US registry is and ought to be "a national public resource" (cite, PDF). In this context, evaluation of .US's registrations to date may properly examine registration trends with an especially detailed level of scrutiny. Registrations like those of Silver Back Corp of Antigua and Barbuda (834 .US domains including `all-animalsex.us` and `alyssa-milano-naked.us`) may come into question for disputed compliance with .US nexus requirements. In addition, while the resale of domains is permissible under .US registration rules, those who register hundreds or thousands of names for the purpose of resale may also find their actions controversial.

The author knows of no proactive enforcement of .US registration restrictions, and it is therefore perhaps not surprising to find many thousands of domains that may be inconsistent with registration restrictions. Consistent with the author's prior investigations of .NAME and .BIZ, compliance with stated registration restrictions seems to require an active and proactive enforcement mechanism; merely demanding that registrants certify compliance with stated rules may not suffice to ensure compliance. Of course, effective enforcement may be difficult and costly; indeed, it may be sufficiently difficult and costly that the Neustar registry and the US Department of Commerce on balance decide against such enforcement. Nonetheless, if current registration restrictions reflect an explicit policy decision as to proper usage of the .US TLD, current enforcement systems may be ineffective at carrying out this policy. Were the DoC and Neustar to remain committed to the current registration restrictions, they might put into place special checks for those registrants outside the US. For example, a first-time non-US .US registrant could be required to fill out a web form detailing its US activities and/or US offices or facilities, the factors considered under Neustar's current statement of Nexus Requirements.

Future work might consider the following questions:

- Change over time, including changes in registration rate, registrar market share, domain usage, and registrations by non-Americans
- Transfers, drops, and other future uses of domains currently held by large registrants
- Renewal rates, and differences in renewal rates across sponsoring registrars
- Search engine listings, and differences in listings across sponsoring registrars
- The extent to which generic .US registrations are held by the same firms that hold the corresponding domains in other TLDs
- The extent to which some large registrants have registered the trademarks of other entities

Thanks to Bret Fausett for suggesting this project and to Tim Hewitt of myOstrich Internet for information on .US sunrise registration restrictions. Thanks also to an anonymous registrar that provided a current .US zone file.

Ben Edelman
Last Updated: September 20, 2002 - Notify me of major updates and additions to this page.
